Gobernación MAGDALENA

E.S.E. HOSPITAL NÚESTRA SEÑÓRA DEL CARMEN
DEPARTMENTO DEL MAGDALENA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA: 2026

MADELEINE FRANCO DÍAZ
Gerente

E.S.E. HOSPITAL NUESTRA SEÑORA DEL CARMEN — *GUAMAL*, MAGDALENA

TABLA DE CONTENIDO

1. INTRODUCCIÓN
2. MARCO ESTRATÉGICO INSTITUCIONAL
   2.1 Misión
   2.2 Visión
   2.3 Valores Institucionales
   2.4 Objetivos Estratégicos Institucionales
3. OBJETIVOS DEL PLAN
   3.1 Objetivo General
   3.2 Objetivos Específicos
4. MARCO NORMATIVO Y DE REFERENCIA
5. DIAGNÓSTICO INSTITUCIONAL
   5.1 Contexto institucional
   5.2 Sistemas de información institucionales
   5.3 Gestión de la confidencialidad
   5.4 Gestión de la integridad
   5.5 Gestión de la disponibilidad
   5.6 Gestión de accesos
   5.7 Gestión de incidentes
   5.8 Componente humano
   5.9 Cumplimiento normativo
   5.10 Articulación con MIPG y Control Interno
   5.11 Nivel de madurez institucional
6. ANÁLISIS DOFA
   6.1 Fortalezas
   6.2 Debilidades
   6.3 Oportunidades
   6.4 Amenazas
7. PLAN DE ACCIÓN
8. MATRIZ DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
9. ARTICULACIÓN CON FURAG
10. SEGUIMIENTO Y EVALUACIÓN DEL PLAN
11. APROBACIÓN Y VIGENCIA.
12. TABLAS Y ANEXOS

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
E.S.E. Hospital Nuestra Señora del Carmen
Guamal, Magdalena
Vigencia 2026

1. INTRODUCCIÓN

La gestión de la seguridad y privacidad de la información constituye un componente estratégico para las entidades públicas del sector salud, en especial aquellas que administran información sensible relacionada con la atención de los usuarios, la historia clínica, los datos personales, la gestión administrativa y financiera. En este contexto, la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, reconoce la información como un activo crítico cuya protección resulta fundamental para garantizar la continuidad del servicio, el cumplimiento normativo y la confianza de la comunidad.

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026 se formula como una herramienta técnica e institucional orientada a identificar, analizar, evaluar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad, en concordancia con los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI, la Norma ISO/IEC 27001 y el Modelo Integrado de Planeación y Gestión – MIPG.

Este plan responde a la necesidad de fortalecer la gobernanza de la información, promover una cultura organizacional orientada a la seguridad digital y articular las acciones institucionales con los requerimientos del Formulario Único de Reporte de Avance de la Gestión – FURAG, generando evidencia objetiva del compromiso de la entidad con la gestión del riesgo y la mejora continua.

Asimismo, el documento se concibe como un instrumento dinámico que permite a la entidad anticiparse a las amenazas, reducir las vulnerabilidades y establecer controles adecuados para proteger la información, contribuyendo de manera directa al fortalecimiento del control interno, la transparencia y la eficiencia administrativa durante la vigencia 2026.

2. MARCO ESTRATÉGICO INSTITUCIONAL

2.1 Misión

La E.S.E. Hospital Nuestra Señora del Carmen presta servicios de salud de primer nivel de atención, con calidad, oportunidad y humanización, contribuyendo al mejoramiento de las condiciones de salud de la población del municipio de Guamal, Magdalena.

2.2 Visión

Ser una institución de salud reconocida por la prestación eficiente, segura y humanizada de los servicios, con procesos fortalecidos, talento humano competente y uso adecuado de las tecnologías de la información.

2.3 Valores Institucionales

Responsabilidad, ética, transparencia, compromiso, humanización y trabajo en equipo.

2.4 Objetivos Estratégicos Institucionales

- Garantizar la calidad y seguridad en la prestación de los servicios de salud.
- Fortalecer la gestión institucional mediante la implementación del MIPG.
- Proteger los activos de información y los datos personales.
- Mejorar la eficiencia administrativa y financiera.
- Promover la cultura del control interno y la gestión del riesgo.

3. OBJETIVOS DEL PLAN

3.1 Objetivo General

Diseñar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la E.S.E. Hospital Nuestra Señora del Carmen para la vigencia 2026, con el fin de mitigar los riesgos asociados a la gestión de la información y fortalecer el cumplimiento normativo e institucional.

3.2 Objetivos Específicos

- Identificar los riesgos que afectan la seguridad y privacidad de la información.
- Definir e implementar controles para el tratamiento de los riesgos identificados.
- Fortalecer la cultura institucional en seguridad de la información.

- Articular la gestión del riesgo con MIPG, MSPI y FURAG.
- Establecer mecanismos de seguimiento y mejora continua.

4. MARCO NORMATIVO Y DE REFERENCIA

El presente plan se fundamenta en la normatividad vigente, entre la cual se destacan: la Constitución Política de Colombia; la Ley 1581 de 2012 sobre protección de datos personales; la Ley 1712 de 2014 de transparencia y acceso a la información pública; el Decreto 1078 de 2015; el Decreto 1499 de 2017; los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI; la Norma ISO/IEC 27001; el Modelo Integrado de Planeación y Gestión – MIPG; y los requerimientos del FURAG.

5. DIAGNÓSTICO INSTITUCIONAL

Seguridad y Privacidad de la Información

La E.S.E. Hospital Nuestra Señora del Carmen administra información de alta sensibilidad, principalmente relacionada con la atención clínica, los datos personales de los usuarios, la información financiera y la gestión del talento humano, lo que exige un enfoque estructurado para la gestión de los riesgos de seguridad de la información.

Actualmente, la entidad cuenta con tres sistemas de información: dos asistenciales (DNA PLUS e INFOSALUD) y uno financiero (APOLO). Estos sistemas operan de manera independiente, sin mecanismos de interoperabilidad, lo que genera riesgos de duplicidad, inconsistencia y pérdida de integridad de la información.

Se evidencia la ausencia de un sistema integral de historia clínica electrónica que garantice la custodia, trazabilidad y control de accesos, situación que incrementa los riesgos legales, operativos y reputacionales para la entidad.

Asimismo, no se cuenta con un responsable formalmente designado para liderar la seguridad y privacidad de la información, lo que limita la gobernanza, la coordinación interinstitucional y la adopción de decisiones estratégicas.

La entidad no dispone de un inventario actualizado de activos de información, ni de una clasificación por niveles de sensibilidad, lo que dificulta la priorización de controles y el tratamiento efectivo de los riesgos.

En materia de gestión de accesos, se identifican debilidades en la definición de roles y perfiles, aumentando la probabilidad de accesos no autorizados y uso indebido de la información.

Desde la perspectiva de disponibilidad, los respaldos de información no se encuentran formalizados dentro de un plan estructurado de copias de seguridad y continuidad del servicio.

En cuanto a la gestión de incidentes de seguridad, la entidad no cuenta con procedimientos formalizados que permitan su identificación, reporte y tratamiento oportuno.

Adicionalmente, se evidencia una baja cultura organizacional en seguridad de la información, derivada de la falta de programas sistemáticos de capacitación y sensibilización.

El diagnóstico permite concluir que la entidad se encuentra en un nivel de madurez inicial a intermedio en la gestión de la seguridad y privacidad de la información, lo que justifica la implementación del presente plan como una prioridad institucional para la vigencia 2026.

6. ANÁLISIS DOFA

Fortalezas: compromiso de la alta dirección, existencia de sistemas de información, marco normativo claro, talento humano dispuesto al cambio, estructura institucional definida.

Debilidades: ausencia de responsable SGSI, sistemas no integrados, falta de inventario de activos, debilidad en controles de acceso, baja cultura de seguridad.

Oportunidades: lineamientos MSPI, evaluación FURAG, avances en gobierno digital, apoyo normativo nacional, fortalecimiento del MIPG.

Amenazas: fuga de información, sanciones legales, ataques cibernéticos, pérdida de información, afectación reputacional.

7. PLAN DE ACCIÓN – PLAN DE TRATAMIENTO DE RIESGOS 2026

Se establece un plan de acción con actividades específicas, responsables definidos, indicadores de gestión y cumplimiento, y cronograma de ejecución, orientado a mitigar los riesgos identificados y fortalecer la seguridad de la información durante la vigencia 2026.

8. MATRIZ DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La matriz identifica los riesgos asociados a la confidencialidad, integridad y disponibilidad de la información, definiendo su impacto, probabilidad, nivel de riesgo y controles de tratamiento, en concordancia con ISO/IEC 27001.

9. ARTICULACIÓN CON FURAG

El plan se articula con los componentes de Gestión del Riesgo, Seguridad Digital, Control Interno, Transparencia y Planeación del FURAG, constituyéndose en evidencia directa del avance institucional en la gestión de la seguridad y privacidad de la información.

10. SEGUIMIENTO Y EVALUACIÓN

El seguimiento al plan se realizará de manera trimestral, con evaluación anual de resultados, permitiendo la adopción de acciones de mejora y el fortalecimiento continuo del sistema.

11. APROBACIÓN Y VIGENCIA

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información rige a partir de su aprobación y tendrá vigencia durante el año 2026, bajo la responsabilidad de la alta dirección y las áreas competentes.

12. ANEXOS

12.1 MATRIZ DOFA

FORTALEZAS (F)	Acciones / Actividades
Compromiso de la alta dirección	1. Formalizar el liderazgo mediante acto administrativo. 2. Aprobar políticas institucionales de seguridad.

	3. Incluir la seguridad de la información en el Comité Institucional. 4. Priorizar recursos para controles críticos. 5. Realizar seguimiento semestral al plan.
Sistemas de información implementados	1. Diagnosticar interoperabilidad. 2. Definir estándares de uso. 3. Unificar criterios de registro. 4. Priorizar activos críticos. 5. Documentar procesos asociados.
DEBILIDADES (D)	Acciones / Actividades
No existe responsable del SGSI	1. Designar responsable formal. 2. Definir funciones y responsabilidades. 3. Capacitar al responsable. 4. Integrar el rol al MIPG. 5. Evaluar su gestión anualmente.
Sistemas no integrados	1. Realizar estudio técnico. 2. Definir requerimientos de integración. 3. Establecer controles de validación. 4. Estandarizar datos. 5. Evaluar soluciones tecnológicas.
No hay sistema integral de historia clínica	1. Definir lineamientos de custodia. 2. Evaluar alternativas tecnológicas. 3. Priorizar la historia clínica como activo crítico. 4. Fortalecer controles manuales. 5. Gestionar recursos para implementación.
OPORTUNIDADES (O)	Acciones / Actividades
Lineamientos MSPI y ISO 27001	1. Adoptar controles recomendados. 2. Alinear políticas institucionales. 3. Capacitar al personal. 4. Fortalecer auditorías internas. 5. Mejorar calificación MIPG.

Evaluación FURAG	1. Generar evidencias documentales. 2. Mejorar respuestas en seguridad digital. 3. Integrar planes institucionales. 4. Fortalecer seguimiento. 5. Formular planes de mejora.
AMENAZAS (A)	Acciones / Actividades
Fugas de información	1. Implementar controles de acceso. 2. Capacitar al personal. 3. Fortalecer políticas de confidencialidad. 4. Gestionar incidentes. 5. Aplicar sanciones disciplinarias.
Sanciones legales	1. Cumplir Ley 1581 y 1712. 2. Documentar controles. 3. Realizar auditorías periódicas. 4. Fortalecer control interno. 5. Implementar acciones correctivas.

PLAN DE ACCIÓNES VIGENCIA 2026

Actividad	Descripción	Indicador de Gestión / Cumplimiento	Responsable	Fecha
1	Designar responsable de seguridad de la información	Acto administrativo expedido	Gerencia	I Trim 2026
2	Actualizar inventario de activos de información	% activos identificados	Sistemas	I Trim 2026
3	Clasificar información institucional	% información clasificada	Sistemas	I–II Trim
4	Implementar controles de acceso	% usuarios con perfil definido	Sistemas	II Trim
5	Definir política de contraseñas	Política adoptada	Sistemas	II Trim
6	Capacitar funcionarios en	% funcionarios capacitados	Talento Humano	II–III Trim

	seguridad de la información			
7	Fortalecer custodia de historia clínica	Procedimiento implementado	Servicios de Salud	II–III Trim
8	Implementar copias de seguridad	Backups periódicos	Sistemas	Permanente
9	Definir procedimiento de incidentes	Procedimiento adoptado	Sistemas	III Trim
10	Articular seguridad con PTEP	Acciones integradas	A.Planeación	III Trim
11	Evaluar riesgos residuales	Informe de evaluación	Control Interno	III Trim
12	Actualizar matriz de riesgos	Matriz actualizada	A.Planeación	III Trim
13	Seguimiento al plan	% actividades ejecutadas	A.Planeación	Trimestral
14	Reporte FURAG	Evidencia cargada	A.Planeación	IV Trim
15	Evaluación anual del plan	Informe final	Control Interno	IV Trim

MATRIZ DE RIESGOS

Riesgo	Causa	Impacto	Probabilidad	Nivel	Control
Acceso no autorizado	Falta de control de accesos	Alto	Alta	Crítico	Perfiles y autenticación
Pérdida de información	Falta de backups	Alto	Media	Alto	Copias de seguridad
Divulgación de datos	Falta de capacitación	Alto	Media	Alto	Sensibilización
Inconsistencia de datos	Sistemas no integrados	Media	Alta	Alto	Validación

ARTICULACIÓN FURAG		
Componente FURAG	**Pregunta / Enfoque**	**Evidencia desde el Plan**
Gestión del Riesgo	Identificación de riesgos	Matriz de riesgos
Seguridad Digital	Protección de la información	Plan de tratamiento
Control Interno	Acciones preventivas	Plan de acción
Transparencia	Protección de datos	Política y controles
Planeación	Seguimiento	Indicadores definidos

NOTIFIQUESE, COMUNIQUESE Y CUMPLASE.

MADELEINE DIAZ FRANCO
Gerente E.S.E Hospital Nuestra Señora del Carmen
Guamal - Magdalena.